LISTING OF CLAIMS

1. (Currently Amended) A method comprising:

~~loading port authentication~~ **executing** firmware instructions [[in]] **to initialize** a supplicant system **into a system management mode (SMM)** during a pre-boot phase;

receiving a network boot request during the pre-boot phase to boot the supplicant system from an operating system (OS) image accessible over a network;

executing port authentication firmware instructions during the pre-boot phase to authenticate ~~ing~~ a network port hosted by an authenticator system and coupled to the supplicant system to which the supplicant system is linked ~~via execution of the port authentication firmware instructions on the supplicant system, wherein the network port is authenticated during the pre-boot phase using~~ **wherein the OS image to boot the supplicant system is accessible through the network port, the authentication firmware instructions to include**

1) **transmitting information identifying the supplicant system to the authenticator system coupled to the supplicant system, and**
2) **transmitting** authentication credentials **to the authenticator system to authenticate the network port coupled to the network;**

booting ~~an operating system~~ **the OS** in the supplicant system **using the OS image accessible over the network in response to the network boot request**;

~~passing the authentication credentials to the booted operating system; and~~

~~using the passed authentication credentials and the booted operating system to perform a port authentication process.~~

executing an OS operation requesting port authentication for the network port; and

executing the port authentication firmware instructions in response to the OS operation request.

2. (Previously Presented) The method of claim 1, wherein the authentication credentials used to authenticate the network port during the pre-boot phase are retrieved from a trusted platform module.

3-6. (Cancelled).

(Currently Amended) 1 /BL/ 6/2/2009

7. ~~(Original)~~ The method of claim ~~6~~, wherein the firmware instructions are embodied as one or more SMM handlers.

8. (Original) The method of claim 7, further comprising:

asserting one of an SMI (system management interrupt) or PMI (Processor Management Interrupt) on a processor of the supplicant on a periodic basis;

dispatching said one or more SMM handlers to handle the SMI or PMI event via operations including,

determining if a network port needs to be authenticated; and, in response thereto, authenticating the network port.

9. (Original) The method of claim 1, wherein port authentication is performed using the EAPOL (extensible authentication protocol over local area network) protocol.

10. (Original) The method of claim 1, wherein the port is authenticated using an access/challenge scheme.

11. (Original) The method of claim 10, wherein the access/challenge scheme employs a Transport Layer Security (TLS) challenge response in which authentication is determined based on credentials provided by the supplicant system.

12. (Original) The method of claim 11, wherein the TLS challenge response employs credentials stored in a Trusted Platform Module (TPM), and wherein the method further comprises retrieving the credentials from the TPM.

13. (Original) The method of claim 1, wherein a determination of whether a port is authenticated is made by an authentication server that is linked in communication with the authenticator system.

14. (Previously Presented) The method of claim 1, further comprising providing a callable interface via which a port authentication process can be invoked.

15-20. (Cancelled)

21. (Currently Amended) A machine-readable ~~media on which~~ **storage medium to store** firmware instructions ~~are stored~~, which when executed by a ~~supplicant system~~ **processor** perform operations including:

~~loading port authentication~~ **executing** firmware instructions [[in]] **to initialize** a supplicant system **into a system management mode (SMM)** during a pre-boot phase;

receiving a network boot request during the pre-boot phase to boot the supplicant system from an operating system (OS) image accessible over a network;

executing port authentication firmware instructions during the pre-boot phase to authenticate ~~ing~~ a network port hosted by an authenticator system and coupled to the supplicant system to which the supplicant system is linked ~~via execution of the port authentication firmware instructions on the supplicant system, wherein the network port is authenticated during the pre-boot phase using~~ **wherein the OS image to boot the supplicant system is accessible through the network port, the authentication firmware instructions to include**

1) **transmitting information identifying the supplicant system to the authenticator system coupled to the supplicant system, and**
2) **transmitting** authentication credentials **to the authenticator system to authenticate the network port coupled to the network;**

booting ~~an operating system~~ **the OS** in the supplicant system **using the OS image accessible over the network in response to the network boot request**;

~~passing the authentication credentials to the booted operating system; and~~

~~using the passed authentication credentials and the booted operating system to perform a port authentication process.~~

executing an OS operation requesting port authentication for the network port; and

executing the port authentication firmware instructions in response to the OS operation request.

22-30. (Cancelled)

31. (New) The machine-readable storage medium of claim 21, wherein the firmware instructions are embodied as one or more SMM handlers.

32. (New) The machine-readable storage medium of claim 21, to store firmware instructions, which when executed by a processor perform operations further including:

asserting one of an SMI (system management interrupt) or PMI (Processor Management Interrupt) on a processor of the supplicant on a periodic basis;

dispatching said one or more SMM handlers to handle the SMI or PMI event via operations including,

determining if a network port needs to be authenticated; and, in response thereto, authenticating the network port.

33. (New) The machine-readable storage medium of claim 21, wherein port authentication is performed using the EAPOL (extensible authentication protocol over local area network) protocol.

34. (New) The machine-readable storage medium of claim 21, wherein the port is authenticated using an access/challenge scheme.

35. (New) The machine-readable storage medium of claim 21, wherein a determination of whether a port is authenticated is made by an authentication server that is linked in communication with the authenticator system.